Jordan K. Cameron (12051)
jcameron@djplaw.com
DURHAM JONES & PINEGAR, P.C.
3301 N Thanksgiving Way, Suite 400
Lehi, Utah 84043
Telephone: (801) 375-6600
Fax: (801) 375-3865

Attorneys for Plaintiff XMission, L.C.

UNITED STATES DISTRICT COURT
DISTRICT OF UTAH, CENTRAL DIVISION

XMISSION, L.C., a Utah company, Plaintiff, vs. DOES 1-20, Defendants.	**COMPLAINT** Case No.: 2:17cv01287 EJF Judge Evelyn J. Furse

COMES NOW Plaintiff XMission, L.C. ("XMission"), and complains and alleges the following:

PARTIES, JURISDICTION AND VENUE

1. Plaintiff XMission is a Utah limited liability company with its principal place of business in Salt Lake City, Utah, and at all relevant times hereto was duly registered and licensed to do business in the State of Utah.

2. Defendants, identified as Does 1-20, are unknown individuals or entities responsible for sending commercial emails in violation of the CAN-SPAM Act. Each of the

Defendants sent emails in conjunction with a company called Clickbank, whose role is presently unknown.

JURISDICTION AND VENUE

3. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1331 (federal question), for violations of the 15 U.S.C. §7701 *et seq.* (CAN-SPAM Act of 2003), and pursuant to 15 U.S.C. § 7706(g)(1) (original jurisdiction) for cases involving a civil action by an internet access service adversely affected by a violation of 15 U.S.C. §7704(a)(1), 15 U.S.C. §7704(b), or 15 U.S.C. § 7704(d), or a pattern and practice that violates subparagraphs (2), (3), (4), and/or (5) of 15 U.S.C. § 7704(a).

4. This Court has personal jurisdiction over the Defendants because the Defendants, and each of them, have purposefully availed themselves of the privileges of conducting commercial activity in the forum state, in part, through the sending of thousands of commercial emails into the state, and the exercise of jurisdiction is reasonable since Defendants should have known that they would be subject to the jurisdiction and laws of the forum state when they sent, or caused the commercial emails to be sent to customers of an email service provider located in Utah.

5. The emails in question evidence Defendants' efforts to target recipients in Utah, including sending thousands of spam emails to email addresses including domains that clearly identify the state of Utah such as [redacted] and approximately 50 others.

6. Additionally, and more specifically, some of the emails in question contain a commonly used spam trick called Bayesian poisoning. Bayesian poisoning exists where the emailer places hidden, nonsensical text in the body of the email in order to confuse spam filters and trick the filters into believing the email is not spam. The Bayesian poisoning in question makes reference to Utah and is an indication that the emailers were targeting Utah. Specifically, it states, "On with circulated and Utah redistributed. to was There constituent civil practice sure map just the firestorm, military the so conservative play said."

7. Venue is proper pursuant to 18 U.S.C. §1391, as a substantial part of the unlawful actions by the Defendants, and each of them, occurred in this judicial district.

GENERAL ALLEGATIONS

8. XMission was founded in 1993 as Utah's first Internet Service Provider ("ISP").

9. From its early days as a private, Utah ISP, to its current role as a global business Internet provider, XMission has expanded its technical offerings to include sophisticated cloud hosting, web hosting, email service and hosting, collaboration tools, business VoIP phone service, and high speed internet connectivity solutions including optical Ethernet, copper and fiber.

10. Throughout its history, XMission has also worked with hundreds of Utah's nonprofit organizations by providing free web hosting services, and by sponsoring a variety of community-based events and facilities.

11. XMission is a widely known and well-recognized ISP in Utah.

12. XMission owns all the servers, routers, and switches on its network through which it hosts and provides its Internet access services for its customers.

13. XMission has an expansive network and infrastructure, which it has had to consistently update, upgrade and augment in order to combat ongoing spam problems.

14. XMission is the sole owner of all its hardware, and has complete and uninhibited access to, and sole physical control over, the hardware.

15. As a legitimate and leading ISP, XMission is a bona fide Internet Access Service ("IAS") as that term defined under 15 U.S.C. §7702(11), 47 U.S.C. §231(e)(4).

16. XMission provides Internet access services to both commercial and residential customers.

17. The email accounts hosted and served by XMission include email accounts owned by third-party customers of XMission, email accounts owned by employees and/or customers of XMission's third-party customers, email account owned by employees of XMission, and also email accounts owned by XMission itself.

18. For purposes of this Complaint, spam is defined as commercial electronic mail messages ("email") that violate the CAN-SPAM Act in one or more ways.

19. Between 2015 and 2017, the unknown Does collectively sent approximately 105,177 emails to XMission's servers in Utah and directed at XMission's customers.

20. Each of the emails contains a common thread, a tracking link that includes the domains clickbank.com and/or clickbank.net.

21. On information and belief, many, if not all, of the emails in question are unlawful spam.

22. The spam emails independently and collectively adversely affected XMission, and independently and collectively contributed to an overall spam problem suffered by XMission.

23. Each of the Doe Defendants is an "initiator" of the spam emails messages as they either transmitted or procured the transmission of the emails in question as such term is defined in 15 U.S.C. § 7702 and 7706(g)(2).

24. Some of the Doe Defendants may also qualify as a "sender" of the spam emails as defined in 15 U.S.C. §7702(16) as they either transmitted or procured the transmission of the emails in question and as their product, service or website is promoted by the emails.

25. On information and belief, the Defendants individually or acting in concert with each other, sent additional spam emails that XMission has been unable to connect directly with them due to the misleading nature of the information in the emails.

26. Each of the emails is a commercial message and contains commercial content.

27. The emails, and each of them, were received by XMission on its mail servers located in Utah.

28. Throughout its business, XMission has expended well in excess of $3,000,000 in hardware acquisition, maintenance and related expenses to increase capacity to deal with increased Spam and related harm, spam filtering expenses, and employee time in dealing with problems caused by its receipt of Spam generally.

29. XMission expends approximately $100,000 to $200,000 per year in dealing with Spam related issues and associated employee time, exclusive of attorney fees.

30. The harm XMission continues to suffer, as the result of its collective spam problem is much more significant than the mere annoyance of having to deal with spam or the process of dealing with spam in the ordinary course of business (i.e., installing a spam filter to discard spam).

31. The harm XMission suffered, and continues to suffer, is manifested in financial expense and burden significant to an ISP; lost employee time; lost profitability; the necessity to purchase and dedicate equipment specifically to process spam that could otherwise be dedicated providing internet access services; harm to reputation; and customer and email recipient complaints relating to spam generally, and at least 26,284 customer reports of spam pertaining to the emails identified herein, which XMission considers as customer complaints.

32. Each of the emails in question violates multiple CAN-SPAM provisions.

33. The majority of commercial emails received by XMission, including the emails in question, violate the CAN-SPAM Act in one or more ways, and contributed to a larger spam problem.

FIRST CAUSE OF ACTION
CAN-SPAM ACT, 15 U.S.C. § 7704(a)(1)

34. Each of the previous paragraphs is realleged herein.

35. The CAN-SPAM Act makes it unlawful to send e-mail messages that contain, or are accompanied by, materially false or materially misleading header Information. 15 U.S.C. § 7704(a)(1).

36. An email header is materially misleading when it impairs the ability of an Internet access service processing the message on behalf of a recipient to identify, locate, or respond to a

person who initiated the electronic mail message or to investigate the alleged violation, or the ability of a recipient of the message to respond to a person who initiated the electronic message.

37. Email headers can be materially misleading in many ways, including as examples when Header Information includes: false sender email accounts; false sender names; false sender email addresses; header information that is registered to unrelated third parties; altered or concealed header information that impairs the ability of a party processing the message to identify or respond to the transmitting party; false WHOIS information; concealed WHOIS information; WHOIS information that that impairs the ability of a party processing the message to identify or respond to the transmitting party.

38. At least 4,039 of the emails in question violate 15 U.S.C § 7704(a)(1) in that the Header Information contained or was accompanied by generic from names and false or misleading header information in the form of false , misleading, incomplete or inaccurate registration information.

39. Header information is also materially false or materially misleading under Section 7704(a)(1) where it contains a generic "from" name and the e-mail is sent from a privacy-protected domain name, or a domain that contains inaccurate of false registration information, such that the recipient cannot identify the transmitting party from the "from" name or the publicly available WHOIS information.

40. At least 29,714 e-mails contained a generic "from" name and originated from a privacy-protected domain. Accordingly, these e-mails violate 15 U.S.C. § 7704(a)(1).

41. The aforementioned accounts for 33,753 violations of 15 U.S.C. § 7704(a)(1).

42. Pursuant to 15 U.S.C. § 7706(g)(3), XMission prays for relief in the amount of $100 per violation of 15 U.S.C § 7704(a)(1).

SECOND CAUSE OF ACTION
CAN-SPAM ACT, 15 U.S.C. § 7704(a)(1)(A)

43. Each of the previous paragraphs is realleged herein.

44. The CAN-SPAM Act makes it unlawful to send email messages that contain, or are accompanied by, materially false or materially misleading Header Information. 15 U.S.C. §7704(a)(1).

45. "Header information that is technically accurate but includes an originating electronic mail address, domain name, or Internet Protocol address the access to which for purposes of initiating the message was obtained by means of false or fraudulent pretenses or representations shall be considered materially misleading." 15 U.S.C. § 7704(a)(1)(A).

46. In order to obtain the domain names from which to send emails, domain registrants are required to provide a name and address to the domain registrar for inclusion in the public WHOIS database.

47. The name and address provided by the domain registrant to the domain registrar constitute material representations.

48. Any email sent from domains registered with false or incomplete names and/or addresses violates of §7704(a)(1)(A).

49. At least 6,762 of the emails in question violate 15 U.S.C § 7704(a)(1)(A) in that the emails were transmitted from domains registered with false, misleading or incomplete contact information.

50. Additionally, an email violates Section 7704(a)(1)(A) where the domain used to send the email was registered (i.e. obtained) or used for a purpose that violates the domain registrar's terms of service.

51. An e-mail sent from such a domain violates the law regardless of whether the email contains a header that is technically accurate.

52. Approximately 42,515 of the emails in question originated from sender domains registered or used for purposes that violate the corresponding registrar's terms of service, despite the fact that the registration and use of the domain was a representation that such would be consistent with the terms of service.

53. The aforementioned accounts for 49,277 violations of 15 U.S.C. § 7704(a)(1)(A).

54. Pursuant to 15 U.S.C. § 7706(g)(3), XMission prays for relief in the amount of $100 per violation of 15 U.S.C § 7704(a)(1).

THIRD CAUSE OF ACTION
CAN-SPAM ACT, 15 U.S.C. § 7704(a)(5)

55. Each of the previous paragraphs is realleged herein.

56. The CAN-SPAM Act requires that every commercial email contain a valid physical postal address of the "sender." 15 U.S.C. § 7704(a)(5)(A)(iii).

57. "Sender" is defined in 15 U.S.C. § 7702(16).

58. Many of the emails pertaining to each Doe Defendant either do not contain any a clearly and conspicuously displayed physical address or do not contain physical address of the "sender" as defined in 15 U.S.C. § 7702(16).

59. Accordingly, XMission prays for relief in the amount of $25 per violation of 15 U.S.C § 7704(a)(5) pursuant to 15 U.S.C. § 7706(g)(3).

FOURTH CAUSE OF ACTION

Aggravated Damages – CAN-SPAM Act 15 U.S.C §7706(g)(3)(C)

60. Each of the previous paragraphs is realleged herein.

61. On information and belief, each of the Defendants committed the violations set forth above willfully and knowingly; or, in the alternative, each of the Defendant's unlawful activity included one or more of the aggravated violations set forth in 15 U.S.C. § 7704(b).

62. Specifically,

a. Defendants knew that they provided false names and addresses in registering domains from which to send emails in order to avoid detection by spam filtering services, law enforcement and private party plaintiffs such as XMission.

b. Defendants knew that they were registering domains to use in a manner that violates registrar policies.

c. Defendant also knew that the physical addresses they provided in the bodies of the emails, if at all, were not the addresses of the "sender" as that term is defined in 15 U.S.C. § 7702(16) and as required by the CAN-SPAM Act.

63. Accordingly, XMission prays for treble damages of the total damage amount determined by this Court.

REQUEST FOR RELIEF

Plaintiff respectfully requests the following relief:

A. Entry of judgment in the amount of $100 per violation of 15 U.S.C. § 7704(a)(1).

B. Entry of judgment in the amount of $100 per violation of 15 U.S.C. § 7704(a)(1)(A).

C. Entry of judgment in the amount of $25 per violations of 15 U.S.C. § 7704(a)(5).

D. Treble damages pursuant to 15 U.S.C. § 7706(g)(3).

E. Attorneys' fees and costs pursuant to 15 U.S.C. § 7706(g)(4).

F. Pre and post-judgment interest at the highest rate permitted by law.

G. Entry of permanent injunction against each Defendant prohibiting each Defendant from sending or causing to be sent email message to XMission and its customers.

H. All other relief deemed just in law or equity by this Court.

DATED this 14th day of December, 2017.

DURHAM JONES & PINEGAR, P.C.

/s/ Jordan K. Cameron
Jordan K. Cameron
Attorneys for Plaintiff

Plaintiff's Address:
51 East 400 South
Suite 200
Salt Lake City, Utah 84111